

同余数判是新定理及其应用

周从尧¹ 陆吉康² 刘周小珏³

1. 湖南大学 北京 100176

2. 中国水利科学研究院 北京 100032

3. 首都经济贸易大学 北京 100124

摘要: 同余数是个千年难题, 在 2019 年后, 中国取得了重要突破, 在同余数判否、同余数判是、同余数求解计算、同余数参数解的群结构、全部解的理论表达等方面都取得了可喜的进步, 在引言小节中我们将会简单列出已有的成果, 本文探讨同余数 A 本身有没有结构, 如果有结构, 结构是什么样子? 本文的定理采用数论的方法, 而且是初等数论的方法。本文发现了多种具有简单结构的无穷序列, 并证明这些序列的每一项均为同余数, 可最有效地生成同余数的序列。同时其理论证明也是最简单的。大大丰富了同余数判是的研究视角。本文利用这些定理, 可以计算得到非常多个同余数的解。

关键词: 同余数; 椭圆曲线; 数论; 代数几何

引言

(1) 公元 2019 年前的同余数判是定理 (01-04)^[1-5].

定理 01: 若 $p \equiv 3 \pmod{4}$, $2p$ 全是同余数, 在千万表中有 174349 个本原同余数

定理 02: 若 $p \equiv 5, 7 \pmod{8}$, p 全是同余数, 在千万表中有 166220+166251 个本原同余数

定理 03: 若 $n \in \mathbb{Z}^+$, 且符合: ① $p_0 \equiv 5, 7 \pmod{8}$ [或 $p_0 \equiv 3 \pmod{4}$] ② $p_i \equiv 1 \pmod{8}$

③ $(p_i / p_0) = -1$ ($i=1 \cdots k$) ④ $(p_i / p_j) = 1$ ($1 \leq j \leq i-1$)

则 $n = p_0 \prod p_i$ [或 $n = 2p_0 \prod p_i$] 是同余数

例题: $11645 = 5 * 17 * 137$, $9078 = 2 * 3 * 17 * 89$, $10591 = 7 * 17 * 89 \cdots \cdots 9923767 = 7 * 17 * 89 * 937$

在千万范围内, 该定理只包含 7873 个本原同余数, 求出其解的只有 118 个。

定理 04: 若 $n \in \mathbb{Z}^+$, 符合 ① $n \equiv 5 \pmod{8}$, ② $p_i \equiv 1 \pmod{4}$, ③ $h(Q(\sqrt{-n})) \neq 4$ 则 n 是同余数

$n=85$ 时, $p_i \equiv 1 \pmod{4}$, $h(Q(\sqrt{-n}))=4$ 不满足条件③, 此定理对同余数 85 无效

另外 $h(Q(\sqrt{-n}))$ 的计算困难, 参考 [6] 只提供了 $n=-$

151 到 $-199h(Q(\sqrt{-n}))$ 的值。

定理 04 的理论高深, 使用非常困难。我们没有得到千万表中究竟有多少个这样的同余数!

(2) 周从尧, 余未, 汤小宁, 汤小波发现和证明的定理定理编号 01-56, 请参考 [5] 全书, 本文略

1. 同余数的等价定义:

1.1 古典定义

若存在有理数 n 和 m , 使 $m^2 - n$, m^2 , $m^2 + n$ 为等平方数, 则公差 n 为同余数。

1.2 常用定义

三边 x, y, z 均为有理数的直角三角形的面积 $n=xy/2$ 叫同余数。

1.3 近代定义

若椭圆曲线 $y^2 = x^3 - n^2x$ 有 $y \neq 0$ 的有理数解, 则 n 为同余数。

2. 判是新定理及其求解,

2.1 基础准备

定义 $uvst$, 表达式 $st(s^2 - t^2)$ 的值全部是同余数。

$st(s^2 - t^2)$ 的公式编号 (00)

我们主要利用此定义及其各变种计算方法, 花费了不少时间算建立了数据库 Tys_mnt, 并取部分字段作为 tys_000(简

称千万表), 作为检验以下各定理的基础. 本文作者提供如下数据共大家参考: 千万表在共有 3252961 个基原同余数, 已经求得该同余数其解的有 156992 个. 在 [5] 的第 13 章提出了十个新算法, 求得了一些极难计算的同余数的解, 如: 101, 103,

127, 157, 173, 191, 197, 223, 229, 269, 271, 278, 293, 302, 303, 311, 317, 334, 359 等, 其 s, t 均超十进 16 位. 其中 157 的结果由查吉尔 (Zagier) 求出, s, t 均为十进 24 位, 同余数 293 的解

由 [5] 求得, $s=15705303325706301534145925, t=14764613336211576651809284$, 计算时间应为 157 的几千倍到一万倍. 众所周知, 任何计算方法必须使用一、二重循环, 当循环变量或中间变量超过一定范围时, 必须用高精度加减乘除及开方, 运算量极其巨大, 有时求某一个同余数的解, 即使用 [5] 中的新方法, 用微机也得几个月甚至数年时间. 至今 400 内还有 5 个同余数的解没有攻克, 它们是 263, 277, 367, 373, 389 见 [5]13 章 16 章. 该法产生的同余数, 模 8 剩余类均有.

2.2 新定理及其运用

定理 uv57: $u^4 - v^4$ 全是同余数 (u 越大解越多, 全是同余数! 只是千万表太小, 花费时间太长)

证明: 在公式中 (00) 中, 令 $s = u^2, t = v^2$ 则同余数 $A = u^2 v^2 (u^4 - v^4)$, 去平方因子 $u^2 v^2$ 则可.

$u < 1000$ 产生 50 万个同余数, 表中保存基原同余数 13062 个, 模 8 剩余类均有,

例: $7^4 - 1 = 2400 = 6 * 16^2, \dots, 227^4 - 99^4 = 9996790 * 16^2$ 去平方后为基原同余数, 下同

13062 个算例保存于 uv57.txt $u^4 - v^4$ 的公式编号 (57)

定理 uv58: $A = 2uv(u^2 + v^2)$ 全是同余数.

证明: 在公式 (00) 中令 $s = u^2 + v^2, t = 2uv$

则同余数 $A = (u^2 + v^2)(2uv)(u^2 + v^2 + 2uv)$
 $(u^2 + v^2 - 2uv)$

$= (2uv)(u^2 + v^2)(u + v)^2(u - v)^2$, 去平方因子
 $(u + v)^2(u - v)^2$ 则可

$u < 1000$ 产生 50 万个同余数, 表中基原同余数 13512 个,

模 8 剩余类均有

例: $2 * 4 * 3 * (4^2 + 3^2) = 6 * 10^2, \dots, 2 * 192 * 43(192^2 + 43^2)$
 $= 9987954 * 8^2$

13512 个算例保存于 uv58.txt 中 $2uv(u^2 + v^2)$ 的公式编号 (58)

定理 uv59: $A = 2(u^4 + v^4)$ 全是同余数.

证明: 在公式 (58) 中, 以 m^2 代替 u, n^2 代替 v , 则

$A = 2m^2 n^2 (m^4 + n^4)$ 去平方因子 $m^2 n^2$ 得

$A = 2(m^4 + n^4)$, 再换元为 u, v 则可得: $2(u^4 + v^4)$ 其公式编号为 (59)

$u < 1000$ 产生 50 万个同余数, 表中基原同余数 1492 个, 只有模 8 余 1, 2, 分为两个小定理:

Uv59A: u, v 奇 奇 时 $A \equiv 1 \pmod{8}$, 730 个例子, 如: $(3, 1) = 41 * 2^2, \dots, (273, 121) = 9980849 * 34^2$

Uv59B: u, v 一奇一偶, $A \equiv 2 \pmod{8}$, 762 个例子, 如
 $(2, 1) = 34 * 2^2, \dots, (4, 3) = 194 * 2^2$

本方法产生了一个新现象, 千万表中用 s, t 方法长期未得其解的同余数, 用 uv59 的方法居然求出该同余数的解, 这样的情况有 667 处, 其中之一: 同余数 $55618 = 2 * 27809 = 2 * p_1$ 的情况 (27809 为模 8 余 1 的素数, 世界上还没有关于 $2 * p_1$ 的判断定理), 简记为 $(s, t, u, v, F) =$

$(?, ?, 395, 92, 937)$ 如何从 uv59 的 u, v 直接转换为 s, t 值得研究。

1492 个结果保存于 uv59.txt

定理 uv60: $A = u^4 + v^4 + 6u^2 v^2$ 全是同余数. $u > v$

证明: 在公式 (57) 中令 $u = m^2 + n^2, v = 2mn$ 则 $A = (u + v)$

$(u - v)(u^2 + v^2) =$

$= (m + n)^2 (m - n)^2 ((m^2 + n^2)^2 + (2mn)^2)$
 $= m^4 + n^4 + 6m^2 n^2$, 换元得

$u^4 + v^4 + 6u^2 v^2$ 公式编号为 (60)

$u < 1000$ 产生 50 万个同余数, 千万表中 1484 个, 已证只有模 8 余 1, 2. 分为两个小定理:

uv60A: u, v 一奇一偶时, $A \equiv 1 \pmod{8}$, 772 个例子.

如: $(2,1)=41, \dots, (197,76)=9980849 \cdot 17^2$

uv60B:u,v 奇 奇 时, $A \equiv 2(\text{mod}8)$, 712 个 例 子 .

如: $(3,1)=34 \cdot 2^2, \dots, (21,5)=226 \cdot 34^2$

本方法也产生了一个新现象, 千万表中用 s,t 方法长期未得其解的同余数, 用 uv60 的方法居然求出该同余数的解, 这样的情况有 656 处, 部分与 uv59 具有相同的同余数, 其中之一: 凑巧也有同余数 $55618=2 \cdot 27809=2 \cdot p_1$, 简记为 $(s,t,u,v,F)=(?, ?, 487, 303, 1874)$

与 uv59 的解的形式不相同, 不同方法可能会产生不同形式的解 (s,t,u,v,F) , 如何从 uv60 的 u,v 直接转换为 s,t 值得研究。

1484 个结果保存于 uv60.txt

定理 uv61: $|u^4 + v^4 - 6u^2v^2|$ 全是同余数 .

证 明 : 在 公 式 (58) 中 令 $s=x=|m^2 - n^2 + 2mn|$, $t=y=|m^2 - n^2 - 2mn|$

则 $x^2 + y^2 = 2z^2$, 其中 $z = m^2 + n^2$

则 $(58) = 2 \cdot |m^2 - n^2 + 2mn| \cdot |m^2 - n^2 - 2mn| \cdot (x^2 + y^2) =$

$|m^4 + n^4 - 6m^2n^2| \cdot (2 \cdot 2z^2)$ 去掉平方因子得

$|m^4 + n^4 - 6m^2n^2|$

换元后得 $|u^4 + v^4 - 6u^2v^2|$ 公式编号 (61)

$u < 1000$ 产生 50 万个同余数, 表中只保存了 2720 个, 已证同余数 A 只有模 8 余 1,7

例: $|13^4 + 6^4 - 6 \cdot 13^2 \cdot 6^2| = 23 \cdot 17^2, \dots, |244^4 + 43^4 - 6 \cdot 244^2 \cdot 43^2| = 9991217 \cdot 17^2$

2720 个同余数例题保存在 uv61.txt

定理 uv62: $u(u+1)(u+2)$ 全部是同余数 .

证明: 在公式 (00) 中令 $u+1, t=1$ 则可 公式编号 (62)

$u < 3$ 万产生 3 万个同余数, 表中只保存了 1302 个, 模 8 剩余类均有

例: $1 \cdot (1+1)(1+2) = 6 \cdot 1^2, \dots, 3508 \cdot 3509 \cdot 3510 =$

$9918870 \cdot 66^2$, 例题保存于 uv62.txt

定理 uv63: $(u^2 + 1)(u^2 + 2)$ 全是同余数

证明: 在公式 (62) 中, 将 u 换元为 u^2 则可 . 公式编号为 (63), 算例保存于 uv63.txt

$u < 3000$ 产生 3000 个同余数, 表中 98 个, 模 8 余 2,6, 已验证模 8 余 123567 的均有 .

例: $(2^2 + 1)(2^2 + 2) = 30 \cdot 1^2, \dots, (56^2 + 1)(56^2 + 2) = 9843906 \cdot 1$

定理 uv64: $u(u^2 + 1)(u^2 + u + 1)$ 全是同余数 .

证明: 在公式 (00) 中, 令 $s = u^2 + u + 1, t = u$ 则可, 公式编号 (64), 例题保存于 uv64.txt

$u < 1200$ 产生 1200 个同余数, 千万表中只保存了 37 个, 已有模 8 余 1,2,3,5,6,7,

例: $18 \cdot (18^2 + 1)(18^2 + 18 + 1) = 182 \cdot 105^2, \dots, 23(23^2 + 1)(23^2 + 23 + 1) = 6741070 \cdot 1^2$

定理 uv65: $(u^4 + 1)(u^4 + u^2 + 1)$ 全是同余数 .

证明: 在公式 (64) 中, 将 u 换元为 u^2 则可 . 公式编号为 (65), 算例保存于 uv65.txt

$u < 80$ 产生 80 个同余数, 由于数值飞快增长, 千万表中只保存了 7 个,

已有模 8 余 1,5,6; 已经验证模 8 余 123567 均有 .

例: $(3^4 + 1)(3^4 + 3^2 + 1) = 7462 \cdot 1, \dots, (8^4 + 1)(8^4 + 8^2 + 1) = 5887302 \cdot 1,$

定理 uv66: $(u+1)(u+2)(2u+3)$ 全是同余数 .

证明: 在公式 (00) 中令 $s=u+2, t=u+1$ 则可, 公式编号 (66) $u < 10000$ 产生 10000 个同余数, 千万表中只保存了 747 个, 模 8 剩余类均有

例: $(23+1)(23+2)(2 \cdot 23+3) = 6 \cdot 70^2, \dots, (1753+1)(1753+2)(1753 \cdot 2+1) = 9918870 \cdot 33^2$

747 个算例保存于 uv66.txt

定理 uv67: $A=u(u^2+3u+1)(u^2+4u+1)$, 全是同余数.

证明: 在公式 (00) 中令 $s=u^2+3u+1$, $t=u$ 则可, 公式编号 (67)

$u<1000$ 产生 1000 个同余数, 只保存了 33 个, 模 8 剩余类均有

$$\text{例: } 4*(4^2+3*4+1)(4^2+4*4+1)=957*2^2$$

例: $8*(23^2+3*23+1)(23^2+4*23+1)=8569294*1^2$, 33 个例题保存于 uv67.txt

定理 uv68: $A=(u+1)(u^2+4u+8)(u^2+5u+9)(u^2+6u+10)$, $u \geq 0$ 全是同余数

证明: 在 (00) 中令 $s=u^2+5u+9$, $t=u+1$ 则可, 公式编号 (68)

$u<180$ 产生 180 个同余数, uv68.txt 中只保存了 19 个, (原因是千万表太小了, A 增长太快)

已有模 8 余 1,2,5,6,7; 已经验证模 8 余 123567 均有.

例: $u=1$, 代入本定理的公式 $A=6630*1^2$, $\dots, u=35$, 代入本定理的公式 $A=9672785*102^2$

定理 uv69: $A=(2u+3)(u^2+5u+7)(u^2+7u+10)(u^2+9u+13)$, $u \geq 0$ 全是同余数

证明: 在 (00) 中令 $s=u^2+7u+10$, $t=2u+3$ 则可, 公式编号 (69), 例题保存于 uv69.txt

$u<150$ 产生 150 个同余数, uv69.tx 中只能保存了 15 个 (表太小了, A 增长太快),

已有模 8 余 1,2,3,5,6; 已经验证模 8 余 123567 均有.

例: $u=3$ 代入公式 $A=310*42^2$, $\dots, u=5$, 代入公式 $A=4305210*1^2$

定理

uv70A: $u^k+2u+1-u^k+3u+1*u^k+4u+1$, $u>1, k>0$ 时全部为同余数

证明: 在公式 (00) 中令 $s=u^k+3u+1$, $t=u$ 则可, 公式编号 (70), 算例保存于 uv70_?.txt

以下为方次 $k=1-5$ 的结果

1 u 到 1600, 得到 76 个同余数的解 其中

$u=28, A=9480135*2^2$; 已有模 8 剩余类 123567

2 u 到 130, 得到 33 个同余数的解 其中

$u=23, A=8569294*24^2$; 已有模 8 剩余类 123567

3 u 到 30, 得到 6 个同余数的解, 其中 $u=5$,

$A=874905*4^2$; 已证模 8 剩余类均有.

4 u 到 14, 得到 3 个同余数的解, 其中

$u=3, A=141141*4^2$; 已证模 8 剩余类均有.

5 u 到 9, 得到 4 个同余数的解, 其中

$u=5, A=45370*1848^2$; 已证模 8 剩余类均有

定理 uv71: $A=u^4-1$ 全为同余数, u 到 2000, 得 162 个同余数, 已有模 8 余 1,2,3,5,6,7

证明: 本定理是 uv57 当 $v=1$ 时的一个子集, 主要用来说明判定定理的表达式可以很简单.

例题: $u=7, A=7^4-1=6*20^2, \dots, u=159, A=9986390*8^2$

定理 uv72: $A=2u(u^2+1)$ 全为同余数, u 到 2000, 得 640 个同余数, 已有模 8 余 1,2,3,5,6,7

证明: 本定理是 uv58 当 $v=1$ 时的一个子集, 主要用来说明判定定理的表达式可以很简单.

例: $u=7, A=2*7*7^2+1=7*10^2, \dots, u=793, A=9973561*10^2$, $s=0, u>0$ 者 46 个.

定理 uv73: $A=2(u^4+1)$ 全为同余数, u 到 2000, 表内得 60 个同余数, 模 8 只能余 1,2

证明: 本定理是 uv59 当 $v=1$ 时的一个子集, 主要用来说明判定定理的表达式可以很简单.

当 u 奇时, 同余数模 8 余 1; 实例 35 个; u 偶时, A 模 8 余 2, 实例 25 个

例: $u=3, A=2(u^4+1)=2(81+1)=41*1^2 \dots u=65, A=8925313*2^2$, $s=0, u>0$ 者 7 个

定理 uv74: $A=(u^4+6u^2+1)$ 全为同余数, u 到 2600, 表内得 78 个同余数的解, 模 8 余 1,2

证明: 本定理是 uv60 当 $v=1$ 时的一个子集, 主要用来说明判定定理的表达式可以很简单.

当参数 u 奇时, A 模 8 余 2; 实例 31 个; u 偶时, A 模 8 余 1,

在录实例为 47 个.

例 : $u=2$ 时 , $16+24+1=41*1^2 \cdots u=79$ 时 ,
 $A=9746882*2^2$, $s=0, u>0$ 者 14 个

定理 uv75: $A = |u^4 - 6u^2 + 1|$ 全为同余数 , u 到 2666, 表
内得 94 个同余数的解 , A 模 8 余 1,7

证明: 本定理是 uv61 当 $v=1$ 时的一个子集, 主要用来
说明判是定理的表达式可以很简单.

例 : $u=9, A = |6561 - 6*81 + 1| = 31*14^2$

例 : $u=205, A=9009431*14^2 \cdots u=207, A=9366223*14^2$

定理 uvKL: 令 $s=K u^2, t=L v^2$, 则 $KL(K^2 u^4 - L^2 v^4)$
全为同余数. 只要 $(K,L)=1, K>L, u>v$ 则可.

证明: 在公式 (00) 中令 $s=K u^2, t=L v^2$ 则可, 通过本定
理更说明了判是定理公式个数的无穷性.

u 算到 1000, 得 50 万个, 记录 2198 个. 例 (8,1,2,1,6), 表
示 $s=8, t=1, u=2, v=1, F=6, A=14*6^2$

例 : 102 (50,1,5,1,35), 表示 $s=50, t=1, u=5, v=1, F=35$ 即
 $102*35^2$ 只有模 8 余 2,6.

总结: 同余数判是有无穷多方法, 方法不同则解的形式
可能不同. 同余数判是定理永无止境.

2.3 主要应用程序

2.3.1 二重循环搜索方法

Clea:@6,10 say date():@6,20 say time() && 程序名:
tuvxx

Use tys_000 && 基础千万表全部记录、部分字段的副本

Repl all u with 0,v with 0,pf with 0,lx with 0 && 保留了有
用字段 Rn,M8 等的内容

J1=0

For uu=2 to 500:@10,10 say uu

For vv=1 to uu-1

$N9=u^4-v^4$ && 定理 uv00 的公式, 每个定理的公

式要做相应的改变再计算

N01=qpf_(n9) && 函数过程, 如 qpf_(500)=5

if n01<1e7: go n01 && 记入千万表

if lx=0

repl all u with uu,v with vv,pf with sqrt(N9/N01),lx with 1

@10, 60 say j1

endi

endi

Endf

Endf:copy to uv57 for u>0 sdf && 只保留有关记录

retu

2.3.2 一重循环算法

clea && 一重循环程序 (uv62-75)

clos data:@6,10 say date():@6,20 say time()

@6,40 say ' ** 程序 :tuvxx_1 库 :tys_001 to uv70_3 ** '

&&70_k, 根据算法作相应修改

use tys_001: repl all u with 0,v with 0,pf with 0,lx with 0

j1=0:j2=0:uvf= ' ' :@10,40 say j1

for x=2 to 30: @10,10 say x

$xk=x*x: n9=x*(xk+2*x+1)*(xk+3*x+1)*(xk+4*x+1)$

&&k=1,...,5, 此句随算法修改

n01=qpf_(n9) && 去平方因子

if n01<1e7: go n01

if lx=0 && lx=0 自由行

repl u with x,v with 0,lx with 1,pf with sqrt(n9/

n01):j1=j1+1:@10,40 say j1

endi

endi

endf

?uvf

Retu

表 1 已经存在的四个判是定理的情况分析表

定理编号	定理简述	预测个数	得解个数	说明
定理 01 见引言 1.1	$p \equiv 3 \pmod{4}$, $2p$ 全是同余数, 如 278 的解 s, t 达十进 24 位	预测多达 174349 个 但是很难求出其解	多年仅得 83 个解	计算求解 非常困难!
定理 02 见引言 1.1	$p \equiv 5, 7 \pmod{8}$, p 全是同余数 如 293 的 s, t 达十进 26 位	预测 332451 个, 但是很难求出 其解	多年仅得 41+388 个	计算求解 非常困难!
定理 03 见引言 1.1	$p_0 \equiv 5, 7 \pmod{8}$ [或 $p_0 \equiv 3 \pmod{4}$], $p_i \equiv 1 \pmod{8}$, $(p_i / p_0) = -1 (i=1 \cdots k)$ $(p_i / p_j) = 1, 1 \leq j \leq i-1$, 则 $n = p_0 \prod p_i$ [或 $n = 2p_0 \prod p_i$] 为同余数	千万范围内预测 7873 个. 需因 子分解并需多次计算勒让德函 数.	118 个解	10^7 内有 3252961 个同余数, 理论高深, 计算困难.
定理 04 见引言 1.1	$n \equiv 5 \pmod{8}$, 因子 $p_i \equiv 1 \pmod{8}$, $h(Q(\sqrt{-n})) \neq 4$, 则 n 为同余数. 理论高深, 证明困难, 使用非常困难.	预测较多, 与定理 02 有重合. 同 时 $h(n)$ 的计算非常困难, $h=4$ 的 例子很少	很难求解 个数不祥	85 为一疑例, 用 h 来判别同 余数的 是或否有隐患.

以上为 2019 年底, 国内外所具有四个判是定理。

参考文献:

- [1] 潘承洞, 潘承彪. 初等数论 [M]. 北京大学出版社, 2013
- [2] 颜松远《椭圆曲线》, [M] 大连理工大学出版社 35-43 (2011.05)
- [3] 冯克勤 "Non-Congruent and Rank Zero Elliptic Curve", [M] 中国科技大学出版社
- [4] 管训贵《同余数的一个充要条件》, [J] 唐山学院学

报, 2009, 22 (6) 7-7

- [5] 周从尧, 余未, 汤小宁, 汤小波. 千年难题同余数的前世今生 [M], 湖南大学出版社, 2023/08
- [6] 田志勇 《关于二次域类数研究》 <https://www.docin.com/p-1107192304>

作者简介:

周从尧 (1944—), 男, 教授, 研究方向: 数论, 概率统计, 计算方法, 椭圆曲线, 组合数学, 复二次域计算。